State of Minnesota Firewall Rule Update Questions

1. What is the security policy that specifies how source, destination, and service in the rule base are to be treated?

   DEED is currently developing policies regarding rule base, but for rule base optimization, DEED will emphasize "tightening" up rules to limit only required and necessary source, destination, and services.

2. If there is no security policy how will the changes and deletions to the rule base be enforced?

   DEED is currently developing policies regarding rule base.

3. Has a rule cleanup ever been attempted before, if so what were the results?

   No rule cleanup has been attempted before at DEED. Our current firewalls are an accumulation of rules and policies dating back seven or eight years. Rules were added as need arose, and these firewalls have also been "managed and administered" by third party outside of DEED. DEED is at the point to reorganize and correct rule base issues.

4. Does accurate documentation exist on IP's in the rule base? If the vendor has to request information from others will the vendor receive the information in a timely manner? i.e. 24 hours.

   DEED does have accurate IP documentation. However, vendor will be working closely with DEED staff on rule base analysis and interpretation.

5. Total number of firewalls in both stand alone and HA configuration.

   Eight Firewalls in Four Clusters

6. Approximate number of rules and NAT's on each firewall.

   307 Total Rules on Four Clusters
   540 Total NATs on Four Clusters

7. Number of objects on each firewall.

   1625 Total Objects on Four Clusters

8. Number of policies on each firewall.

   One policy for three clusters

One policy for fourth cluster

9. Is there a naming standard for hosts or network objects created or being created?

DEED does have a current naming standard, but DEED does require modification of standard.

10. Who owns the IP Schema for the project?

DEED owns all private and internal IP Networks
State of Minnesota, OET, owns all public IP Networks

11. What are the IPSO and Checkpoint versions on the firewalls?

All Firewalls will be upgraded before we begin any Rule Base Optimization. Final Firewall Configuration will consist of following:

Cluster One – Checkpoint UTM 5070, R70
Cluster Two – Checkpoint UTM 1070, R70
Cluster Three – Checkpoint UTM 1070, R70
Cluster Four – Nokia IP360 (IPSO Version tbd), Checkpoint R65 or R70 (tbd)

12. What platforms are in use by the firewalls, i.e. Nokia, SPLAT, etc?

Nokia and Splat

13. Is SecureXL being used?

No

14. Is SmartDefense being used?

No

15. How is the network managed, internally or outsourced.

Internally, by DEED, with outside consultant help for major upgrades or as needed.

16. Are they managed by P1 or CAM only?

DEED is not using P1 or CAM.

17. What kind of network access to the firewall objects will the vendor have? Will he be on the inside or have to go through a firewall to reach the objects.

Vendor will be working directly with DEED Staff, working from the Internal network. Access rights to be determined and will depend on function being performed.

18. If the vendor has to go through firewalls will rules be in place on each firewall to allow access.

Full access to all firewalls is available.

19. What is considered an "unused rule" no activity within what period of time.

To be determined during next firewall rule set review.

20. Assumption, if an unused rule is disabled or deleted, and its corresponding NAT, if there is one, will be disabled or deleted.

Yes, NAT will also be disabled or deleted.

21 If an "unused rule" is to be removed or disabled is a change request required, and if so what's the length of time it takes to get a change request approved.

We will not be using Change Requests for Rule Base Optimization; vendor will be working directly with DEED Staff to make determination of necessary changes.

22. Can one change control request be used to eliminate a quantity of unused rules on different firewalls, or is a separate request needed for each firewall.

N/A

23. Will the business owner of each rule to be disabled or deleted need to signoff before the action can be completed.

Vendor will be working directly with DEED staff to make determination of necessary changes, no business owner signoff.

24. Phase I requires a Windows Server with Eventia be installed to run reports and Checkpoint Visual HTML tool set installed on SmartCenter server to provide viewable objects, groups, nodes, networks and rules. Will it be the vendor's responsibility to install the server?

Vendor will assist DEED staff in Eventia Installation.

25. Phase III calls for the pushing and testing new rules and objects what are the procedures for testing new rules, where will the people come from and how much notice will be required?

A Test Plan and procedures will be developed as part of the rule base analysis and evaluation. Rule base optimization will be a continual process, changing a small number of rules and objects at a time during firewall update.

26. What are the criteria for determining the successful completion of the project?

Successful completion of the project will include;

- Single Drop Rule at end of Rule Base
- Removal of all unneeded and unused Objects
- Removal of all unneeded and unused Rules
- Realignment of Firewall Rules, based on use and analysis, to operate in an optimal manner
- Documentation and notation for rules and objects in the firewall policy
- A procedure for future analysis

27. Can you describe the Check Point firewall architecture in terms of numbers of Management Servers, Log Servers and enforcement points ?

Cluster One – Checkpoint UTM 5070, R70
Cluster Two – Checkpoint UTM 1070, R70
Cluster Three – Checkpoint UTM 1070, R70
Cluster Four – Nokia IP360 (IPSO Version tbd), Checkpoint R65 or R70 (tbd)

Two Firewall Management Servers and One Policy Server

28. How many single firewall enforcement points, or HA firewall enforcement point clusters are within the scope of the DEED Firewall Rule Update and Evaluation Project?

Four clusters

29. Does DEED use a single ‘Enterprise’ firewall policy on the Smartcenter server, and if so how many rules exist in this policy?

DEED uses a single enterprise firewall olicy with:

307 Total Rules on four clusters
540 Total NATs on four clusters

30. What is the average number of rules installed upon each enforcement point, or enforcement point cluster?

The majority of the rules are installed at headquarters firewalls.

31. How many objects reside in the Smartcenter server objects database?

1625 Total objects on four clusters

32. How many IP hosts are protected by the firewall enforcement points, or firewall enforcement point clusters?

DEED has about 350 Windows servers, all residing on Internal network.

33. Approximately how many users PCs are protected by the firewall enforcement points ?

DEED has about 2,700 PC Users and approximately 400 printers that are residing on the Internal network.

34. What are the methods of User Access to the network ?

Ethernet while on site
Citrix VPN for remote access

35. Will further network segmentation, that may require provisioning new firewall interfaces, fall within the scope of the Firewall Rule Update and Evaluation Project?

No further segmentation will be required and therefore not a part of this project

36. Will the vendor have the ability to use tools in addition to Eventia Reporter for firewall rule evaluation?

DEED will evaluate vendor's new toolsets as deemed necessary.

37. Will the vendor have the ability to use network taps, sniffers, protocol analyzers, and make use of any existing network session data?

Yes, DEED will provide the necessary equipment.

38. Is the vendor responsible for procuring all hardware and software for the use of Eventia reporter?

No, DEED will purchase hardware and software, but we would request some help from vendor for Installation and configuration.

39. Where in the proposal response should the work plan be provided? Does the work plan fall under Section 2. on page 4 of the SOW as a discussion of the deliverables?

Yes, to both your questions. Page 4 Section 2: Deliverables is the actual work plan.

40. Where in the proposal response should resumes be provided?

Yes, to both your questions. Page 4 Section 2: Deliverables is the actual work plan.

41. Under Section 1. on page 4 of the SOW, it states "Resource #1 and 2" – are you looking for two candidates or is the number of resources determined by the proposed work plan?

DEED is looking for two candidates but should you have only one that would be acceptable.

42. We currently have the service category ‘Network (Data, Video, Voice) – Application (Design & Development)’ under our master contract. Would we specifically need to have the ‘Network (Data, Video, Voice) – Security and/or Architecture Planning & Assessment’ service category in order to respond to this SOW?

Yes, a vendor must be approved in at least 1 of the service categories listed in the Statement of Work.